

IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF TEXAS  
AUSTIN DIVISION

FILED

2018 MAR 14 PM 1:35

IN THE MATTER OF THE SEARCH OF  
INFORMATION AND RECORDS  
ASSOCIATED WITH MICROSOFT  
SEARCHES FOR VARIOUS SEARCH  
TERMS THAT ARE STORED AT  
PREMISES CONTROLLED BY  
MICROSOFT

Case No.

1:18-mj-171

Filed Under Seal

**AFFIDAVIT**

I, Scott Kibbey being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

I make this affidavit in support of an application for a search warrant for information associated with certain search terms entered into Bing search or Bing Maps that is stored at premises owned, maintained, controlled, or operated by Microsoft, a networking and remote computing service provider headquartered at One Microsoft Way, Redmond, WA 98052-6399. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) and Rule 41 of the Federal Rules of Criminal Procedure to require Microsoft to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the

information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

1. In particular, this application seeks to obtain information from Microsoft associated with the following search terms, as further described in Attachment A (collectively referred to as the "Microsoft Search Terms") or any other applicable variants of the following search terms:

**1112 Haverford Drive, Austin, TX 78753**  
**1112 Haverford Dr, Austin, TX 78753**  
**1112 Haverford Drive, Austin, TX**  
**1112 Haverford Dr, Austin, TX**  
**1112 haverford austin tx**  
**1112 haverford austin**  
**1112 Haverford Drive**  
**1112 Haverford Dr**  
**1112 Haverford**

**4806 Oldfort Hill Road, Austin, TX 78723**  
**4806 Oldfort Hill Rd, Austin, TX 78723**  
**4806 Oldfort Hill Road, Austin, TX**  
**4806 Oldfort Hill Rd, Austin, TX**  
**4806 oldfort hill austin tx**  
**4806 oldfort hill austin**  
**4806 Oldfort Hill Road**  
**4806 Oldfort Hill Rd**  
**4806 Oldfort Hill**

**6706 Galindo Street, Austin, TX 78741**  
**6706 Galindo St, Austin, TX 78741**  
**6706 Galindo Street, Austin, TX**  
**6706 Galindo St, Austin, TX 78741**  
**6706 galindo austin tx**  
**6706 galindo austin**  
**6706 Galindo Street**  
**6706 Galindo St**  
**6706 Galindo**

**6705 Galindo Street, Austin, TX 78741**  
**6705 Galindo St, Austin, TX 78741**  
**6705 Galindo Street, Austin, TX**  
**6705 Galindo St, Austin, TX 78741**  
**6705 galindo austin tx**  
**6705 galindo austin**  
**6705 Galindo Street**

**6705 Galindo St**  
**6705 Galindo**

3. I have been employed as a Special Agent (SA) of the Federal Bureau of Investigation (FBI) since November since 2011. I am currently designated as a Cyber agent assigned to the Austin Resident Agency of the San Antonio Field Office. I have received formal and on the job training in cyber crime investigation techniques, computer evidence identification, and computer evidence seizure and processing. As a Federal Agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I have participated in the execution of numerous search warrants for documents and other evidence, including computers and electronic media, in cases involving crimes the FBI is authorized to investigate. I am a "federal law enforcement officer" within the meaning of Rule 41(a)(2)(C) of the Federal Rules of Criminal Procedure. I am engaged in enforcing federal criminal laws and am authorized by the Attorney General to request a search warrant, among other things.

4. I have participated in the investigation of the offense(s) listed herein. This affidavit is based on my personal knowledge as well as reports made by other law enforcement officers from agencies to include the FBI, Austin Police Department (APD), Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), the U.S. Postal Inspection Service (USPIS), and others. Because this affidavit is being submitted for the limited purpose of establishing probable cause for the issuance of a search warrant, and it does not contain every fact known to me or other agents of the Federal Bureau of Investigation. Additionally, the incidents described herein occurred a short time ago; the investigation is ongoing and in its preliminary stages.

5. The APD, ATF, FBI, USPIS, and other agencies are investigating a series of bombings that occurred in Austin, Texas, which is within the Western District of Texas, in March 2018. Preliminary analysis of the bombings revealed that the explosive device utilized in all three

incidents was a pipe bomb concealed inside of a cardboard box. Those devices are each legally classified as a Destructive Device as defined by Title 26 United States Code § 5845. Title 26 United States Code § 5861 makes it unlawful for any person to possess a firearm ("firearm" is defined as including a Destructive Device) that is required to be registered with the National Firearms Registration and Transfer Record and is not so registered. Title 26 United States Code § 5861 also makes it unlawful to transfer a firearm (including a Destructive Device) to a person to whom the firearm is not registered.

6. The information requested in this Application is being sought by the FBI, in part, to establish who searched for information about the following addresses during the following prescribed times:

**1112 Haverford Dr Austin, TX 78753  
(from February 2, 2018 through March 2, 2018 06:55 a.m. (CST))**

**4806 Oldfort Hill Rd, Austin, TX 78723  
(from February 12, 2018 through March 12, 2018 06:44 a.m. (CDT))**

**6705 Galindo St, Austin, TX 78741  
6706 Galindo St, Austin, TX 78741  
(from February 12, 2018 through March 12 11:50 a.m. (CDT))**

There is probable cause that individuals who searched for these specific addresses during this time period will help law enforcement to identify persons who may have knowledge about the bombings.

7. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

8. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 26 United States Code § 5861 have been committed by an unknown subject. There is also probable cause to search the information described

in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

### **JURISDICTION**

9. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711 and 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **DEFINITIONS**

The following definitions apply to this Affidavit and Attachment B:

10. “Computer” refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” See 18 U.S.C. § 1030(e)(1).

11. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) could assign a different unique IP address to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

12. A User Agent String (UAS) is the text that programs use to identify themselves to servers, such as web servers, for usage tracking and other purposes. A UAS identifies a user’s web browser and provides certain system details to the services hosting the website a user visits that the server uses to provide content back to the user that is tailored to their respective environment. Web browsers collect UAS of all visitors to a webpage in order to provide the visitor a version of the website that is properly formatted for their web browser. A UAS provides details about the hardware

and software the user might be using to visit the webpage such as operations system, web browser version, and occasionally hardware manufacturer of the device used to visit the webpage.

### **BACKGROUND INFORMATION ABOUT MICROSOFT**

13. In my training and experience, I have learned that Microsoft provides a variety of online services, including, but not limited to, Microsoft Search, Bing Maps, mapping services which provide driving directions, and electronic mail ("email") access, to the public. Microsoft allows customers to utilize the mapping service without creating a Microsoft Account but customers can also obtain email accounts at the domain name gmail.com. Microsoft also maintains records of the IP addresses associated with searches conducted on Bing Search and Bing Maps. Subscribers obtain an account by registering with Microsoft. During the registration process, Microsoft asks subscribers to provide basic personal information. Therefore, the computers of Microsoft are likely to contain information concerning users and their use of Microsoft services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

14. In my training and experience, Microsoft generally asks its subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). Such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

15. In my training and experience, Microsoft retains certain transactional information about the creation and use of each account on its systems. Microsoft also maintains transactional information about users who access a Microsoft account. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Microsoft often has records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers, mobile devices, or other electronic devices were used to access the email account

16. As explained herein, information stored in connection with a Microsoft account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element of an offense, or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with a Microsoft account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

17. Further, I know that information maintained by Microsoft can show how and when the account was accessed or used. Microsoft also collects and maintains location information pertaining to an account and the use of various Microsoft services. For example, as described below, Microsoft typically logs the Internet Protocol (IP) addresses from which users access a Microsoft account, along with the time and date of that access, and location data for the device(s) logged into the account. By determining the physical location associated with the logged IP addresses,

investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner, but can also help locate the device that has logged into a Microsoft account.

18. In my training and experience, e-mail providers typically retain sign-in, session state, and site cookies. E-mail providers also retain information linking accounts by sign-in, session state, and site cookies. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

19. Web browsers collect User Agent Strings (UAS) of all visitors to a web page in order to provide the visitor a version of the website that is properly formatted for their web browser. A UAS provides details about the hardware and software the user might be using to visit the webpage; such as operating system, web browser version, and occasionally hardware manufacturer of the device used to visit the web page. These details will aid in identifying persons searching for information in connection with the aforementioned bomb threats.

20. Previous investigations and legal process have confirmed that this information does exist and can be provided with an appropriate court order with a narrow time frame for the requested terms.

21. Therefore, the computers of Microsoft are likely to contain all the material described above, including stored electronic search terms. It is requested that Microsoft provide any IP addresses, User Agent Strings, and associated Microsoft account information as further described in Attachment B, that entered the search terms in Attachment A into Bing search and Bing Maps during the prescribed timeframes.



22. This application seeks a warrant to search all responsive records and information under the control of Microsoft, a provider subject to the jurisdiction of this court, regardless of where Microsoft has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Microsoft's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.<sup>1</sup>

### **FACTS**

23. On March 2, 2018 at approximately 6:55 am, at 1112 Haverford Drive, Austin, Texas 78753, in the Western District of Texas, an explosion occurred on the front porch of the single story brick residence, resulting in the death of Anthony S. House.

24. On March 12, 2018 at approximately 6:44 am at 4806 Oldfort Hill Drive, Austin, Texas 78723, in the Western District of Texas, an explosion occurred inside the residence, resulting in the death of a 17-year old victim and injuries to an additional victim.

25. On March 12, 2018 at approximately 11:50 am at 6706 Galindo Street, Austin, Texas 78741, in the Western District of Texas, an explosion occurred outside of the residence, sending one person to the hospital with injuries. Based on communications from the victim, the package containing the explosive device may have had the address "6705 Galindo" written on it.

---

<sup>1</sup> It is possible that Microsoft stores some portion of the information sought outside of the United States. In Microsoft Corp. v. United States, 2016 WL 3770056 (2nd Cir. 2016), the Second Circuit held that the government cannot enforce a warrant under the Stored Communications Act to require a provider to disclose records in its custody and control that are stored outside the United States. As the Second Circuit decision is not binding on this court, I respectfully request that this warrant apply to all responsive information – including data stored outside the United States – pertaining to the identified account(s) that is in the possession, custody, or control of Microsoft. The government also seeks the disclosure of the physical location or locations where information responsive to this warrant is/are stored.

26. Law enforcement has assessed that the explosive devices shared commonalities, such as the delivery method, contents of the explosive device, and the manner of detonation. Law enforcement believes all three explosions are linked and these incidents may be connected.

27. The Government has not found any information of a registered Destructive Device for any of the victims of these bombings or residence of the homes, making the possession or transfer to them unlawful.

28. Based on my investigative experience, it is very common to search for addresses utilizing search applications like Bing search and Bing Maps to locate and travel to specified addresses. Since the three bombing locations are residences in residential neighborhoods, and not businesses addresses, I believe that the pool of individuals searching for these addresses will be relatively small. By identifying the users of the Microsoft accounts or IP addresses of the devices that searched Microsoft for these addresses and cross-referencing that data with other investigatory steps such as cellular telephone records, a suspect(s) or witness(es) may be identified.


### **CONCLUSION**

Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Microsoft, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant during any time, day or night.

### **REQUEST FOR SEALING**

I further request that the Court orders that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public, nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize this investigation.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

  
\_\_\_\_\_  
SCOTT KIBBEY  
Special Agent  
Federal Bureau of Investigation  
Austin, Texas

Subscribed and sworn to before me at Austin, Texas, on this 14 day of March, 2018.

  
\_\_\_\_\_  
HON. MARK LANE  
UNITED STATES MAGISTRATE JUDGE